| FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE | ATTY DOCKET NO. 20206-25 | SERIAL NO. 09/328,726 |
|---|---|---|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT | APPLICANT Collins | |
| | FILING DATE October 26, 1998 | GROUP 2766 |

## U. S. PATENT DOCUMENTS

| EXAMINER INITIAL | | DOCUMENT NUMBER | DATE | NAME | CLASS | SUBCLASS | FILING DATE IF APPROPRIATE |
|---|---|---|---|---|---|---|---|
| | AA | | | | | | |
| | | | | | | | |

## FOREIGN PATENT DOCUMENTS

| | | DOCUMENT NUMBER | DATE | COUNTRY | NAME | CLASS | SUBCLASS | TRANSLATION YES NO |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

| | | | |
|---|---|---|---|
| ρωk | AB | | *IEEE 1994 Electronics Letters Online No: 19941450 "Using four-prime RSA in which some of the bits are specified"* S. A. Vanstone and R. J. Zuccherat – Electronics Letters 8th December 1994 Vol 30, No. 24, pp. 2118, 2119. |
| ρωk | AC | | *RSA '98 Presentation – F. Levy-dit-Vehel – January 98 "Stuffing An RSA Into The Smallest 68HC05", pp. 1-14.* |
| ρωh | AD | | *Generating a Product of Three Primes With an Unknown Factorization,* Dan Boneh and Jeremy Horwitz, Computer Science Department, Stanford University. |
| ρωk | AE | | *ChipCenter: The Web's Definitive Electronics Resource – "Compaq Computer Corporation – WebScan :Press Release"* (4/11/00) |
| ρωk | AF | | *Newell Public Relations, Hong Kong – "RSA Security teams with Compaq to provide high-speed cryptography breakthrough for manufacturers of wireless and embedded devices" (April 19, 2000)* |
| ρωk | AG | | *Compaq News via WebLibrary – "New RSA BSAFE Crypto-C Encryption Software Offers up to 500 Percent Performance Gains for E-Commerce, Secure E-Mail and Other Applications"* PR News Wire via DowVision (September 6, 2000). |
| ρωk | AH | | *Compaq News via WebLibrary – "RSA Security Releases RSA Encryption Algorithm into Public Domain"* PR News Wire via DowVision (September 6, 2000). |
| ρωk | AI | | *RSA Security – RSA BSAFE\* - Wireless Transport Layer Security for C (8/31/2000).* |
| ρωλ | AJ | : | *CyberLaw Presents: The RSA Algorithm & The RSA Patent – "Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?"* Patrick J. Flinn and James M. Jordan III\*; (c) 1997 Alston & Bird LLP (July 9, 1997). |
| ρωk | AK | ` | *RSA Laboratories / Bulletin 13 (April 2000) "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths"* Robert D. Silverman, RSA Laboratories |
| ρωk | AL | . | *1982 International Symposium on Information Theory;* Les Arcs, France (June 21-25, 1982). |
| ρωλ | AM | . | *Lecture Notes in Computer Science (Edited by G. Goos and J. Hartmanis) – "Advances in Cryptology – CRYPTO '86" Proceedings* |
| ρωk | AN | , | *"An Introduction to Fast Generation of Large Prime Numbers"* by C. Couvreur and J. J. Quisquater; Phillips J. Res. 37, 231-264, 1982 |
| ρωk | AO | . | *"A Method for Obtaining Digital Signatures and Public Key Cryposystems"* R. L. Rivest, A. Shamir, and L. Adelman, MIT Laboratory for Computer Science and Department of Mathematics |
| ρωλ | AP | | *MIT/LCS/TR-212 – "Digitalized Signatures and Public-Key Functions As Intractable As Factorization"* Michael O. Rabin (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science. |
| ρωk | AQ | . | *Permutation Polynomials in RSA-Cryptosystems* Rudolf Lidl and Winfried B. Müller; Department of Mathematics, University of Tasmania, Hobart Australia 7001 and Institut für Mathematik, Universität Klagenfurt, A-9020 Klagenfurt, Austria |
| ρωk | AR | . | *PKCS #1: RSA Encryption Standard – An RSA Laboratories Technical Note, Version 1.5, Revised November 1, 1993* |

| *pwk* | AS | | *High-Speed RSa Implementation* Cetin Kaya Koc, RSA Laboratories RSA Data Security, Inc., 100 Marine Parkway, Suite 500, Redwood City, CA 94065-1031; Copyright © RSA Laboratories Version 2.0 – November 1994 |
|---|---|---|---|

| EXAMINER | DATE CONSIDERED |
|---|---|
| Paula Klimach | 1/11/06 |

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.